Secure CA Gateway

EPICS meeting at SLAC
April 26, 2005
N. Yamamoto
GAN operation scenario
Access to a control system from outside of Lab.

Allow safe access from outside of lab.

- Safe connection to hosts in the control system.
  - VLAN
  - Dedicated Line
  - SSH tunnel from the Internet
  - login to one of CPU in control system.
  - Once user login to the hosts, it is difficult to distinguish access from outside and access from inside lab.

- Allow user to use same tools on their PC/NB.
  - Secure CA:
    - identification: PKI
    - secure connection: SSL
  - Access privilege management
  - Enhance CA gateway to support secure connection: Secure CA Gateway
Secure CA Gateway

Use PKI to identify and authenticate the user
Use SSL for secure connection
Access control management system have to be implemented
  – description of
Assume access from the inside hosts are safe.
Keypoints for secure CA GW

**flexibility**
- Allow to introduce new context.

**transparency**
- Can be introduced without large modification to existing system.

**security**
- Must be secure under remote operation environment.

**performance**
- Keep there performance. or Take a balance with Flexibility, Transparency, security
We need to modify...

CA client library
- Authentication on opening the connection to the server
- SSL support

Gateway
- Authentication using PKI
- SSL support
- Access to privilege control database
  - Query: Channel name and PKI identification, (and access point), as a key.
  - Configuration
  - Change configuration dynamically
    - reserve a set of channels for a particular user/group for modification.